

#### REMARKS

Reconsideration of the application is requested.

Applicants acknowledge the Examiner's confirmation of receipt of applicants' certified copy of the priority document, German patent application DE 101 11 756.6, filed March 12, 2001 supporting the claim for priority under 35 U.S.C. § 119.

Claims 1-21 remain in the application. Claims 1-21 are subject to examination. Claims 1, 12, and 17 have been amended.

Under the heading "Claim Objections" on page 2 of the above-identified Office Action, the Examiner objected to claims 1, 12, and 17 because of informalities.

The Examiner's suggested corrections for claims 12 and 17 have been made. Applicant believes the wording for claim 1 is correct. The acceptance of the data set is dependent on the results of the checking step. However, applicant has amended claim 1 to clarify this point.

Under the heading "Claim Rejections - 35 USC § 112" on pages 2-3 of the above-identified Office Action, claim 1 has been rejected as being indefinite under 35 U.S.C. § 112, second paragraph.

More specifically, the Examiner notes three antecedent basis issues in claim 1. Claim 1 has been amended to address the three antecedent basis issues.

It is accordingly believed that claim 1 meets the requirements of 35 U.S.C. § 112, second paragraph. The above-noted changes to the claims are provided solely for clarification or cosmetic reasons. The changes are neither provided for overcoming the prior art nor do they narrow the scope of the claim for any reason related to the statutory requirements for a patent.

Under the heading "Claim Rejections - 35 USC § 102" on pages 3-6 of the above-identified Office Action, claims 1-6, 13-16 and 21 have been rejected as being fully anticipated by U.S. Patent No. 5,757,918 to Hopkins (hereinafter Hopkins) under 35 U.S.C. § 102.

As will be explained below, it is believed that the claims were patentable over the cited art in their original form and, therefore, the claims have not been amended to overcome the references.

Hopkins describes communication between a smart card (a prover) and a terminal (a verifier). Authentication is

performed by using a challenge-response-scheme (see column 3, lines 25 - 30). First, the prover generates a random number  $(x)$ , and computes a quantity  $T$  using public keying material  $(e, n)$ .  $T$  is then transmitted to the verifier, which also generates a random number  $y$  (challenge), which is sent to the prover.

The prover further computes a quantity  $S$  from  $x$ ,  $y$ ,  $n$  and private keying material  $(aB)$ . Quantities  $a$  and  $B$  are further related to a public identification  $U$  (see, e.g., equation (1) in column 5, and the relation  $a=P(UP)^d \bmod n$ , wherein  $d$  is a card issuer's private key and  $P$  is the PIN of the card). Prior to computing  $S$ , the private keying material  $(aB)$  is obtained, i.e. decrypted (see column 3, lines 25-31) in the prover using the specific PIN known solely to the user of the smart card.

The prover then sends quantities  $S$  and  $U$  to the verifier. The verifier computes quantity  $T'$  from  $S$ ,  $y$ ,  $U$  and the public key  $(e, n)$ . For mathematical reasons, the prover is authenticated, if computed values  $T$ ,  $T'$  are equal (see column 6, lines 58-60).

In summary, the prover according to Hopkins encrypts number elements  $(x, y)$  for transmission and the verifying element decrypts the messages that it has correspondingly received.

In contrast, step c) of claim 1 of the instant application recites encrypting a data element by the verifier and decrypting it by the prover. Consequently, the invention of the instant application is opposite with respect to Hopkins and therefore believed to be novel.

As a result of this difference, data elements exchanged between the prover and the verifier are communicated in encrypted form according to the invention, and in decrypted form according to Hopkins. Hence, the number elements according to Hopkins cannot be used in further communication as keys. Therefore, Hopkins does not teach method steps for authenticating the prover or the verifier using a symmetrical cryptographic scheme (steps (f) - (i) in claim 1 of the instant application). In particular, having performed the method steps of Hopkins (column 5, line 11 to column 6, line 56), the prover is authenticated, but the prover does not have a key to encrypt data towards the verifier.

In summary, the features of claim 1 of the instant application are neither shown nor suggested by Hopkins.

Under the heading "Claim Rejections - 35 USC § 103" on pages 7-11 of the above-identified Office Action, claims 7-12 and 17-20 have been rejected as being obvious over Hopkins in view

of U.S. Patent No. 5,272,755 to Miyaji et al. (hereinafter Miyaji) under 35 U.S.C. § 103.

Claims 7-12 and 17-20 ultimately depend on claim 1. Because claim 1 is believed to be allowable, claims 7-12 and 17-20 are also believed to be allowable.

It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claim 1. Claim 1 is, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1.

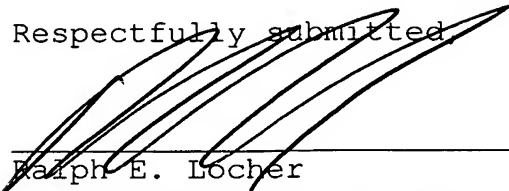
In view of the foregoing, reconsideration and allowance of claims 1-21 are solicited.

If an extension of time is required, petition for extension is herewith made. Any extension fee associated therewith should be charged to the Deposit Account of Lerner Greenberg Stemer, LLP, No. 12-1099.

Please charge any other fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner

Greenberg Stemer, LLP, No. 12-1099.

Respectfully submitted,



---

Ralph E. Locher  
Registration No. 41,947

March 21, 2006

Lerner Greenberg Stemer, LLP  
P.O. Box 2480  
Hollywood, Florida 33022-2480  
Tel.: (954) 925-1100  
Fax: (954) 925-1101